WERKSMANS
ATTORNEYS

REGULATORY

Civil damages or even class action suits a possibility for companies failing to protect customer data

9 October 2019 *4 min read*

by Ahmore Burger-Smidt, Head of Data Privacy Practice

Companies that fail to protect their customers' personal information may face class action suits once the Protection of Personal Information Act (POPIA) comes into force in South Africa.

With the growing threat of cybercrime, companies need to ensure they take data leaks seriously.

Cybercrime is expected to be the most disruptive economic crime to affect organisations over the next 24 months. This is according to a quarter of SA respondents to a 2018 PwC survey.

Another survey, by Refinitiv in 2018, found that 20% of 2 373 global respondents (123 from SA), had suffered loss from cybercrime.

Data fraud and theft and cyber attacks are ranked the 4th and 5th biggest global threats in the next decade by the World Economic Forum.

So the threat of something happening to your customer data is real. Criminals steal customer data to hold the company to ransom for the return of the data, or to use the data to commit fraud or theft.

We have recently seen massive breaches of personal information. Among the largest was in India, where the government ID database, Aadhaar, reportedly suffered data breaches that potentially compromised the records of 1.1 billion citizens.

And these attacks will continue as we grow increasingly dependent on the digital interconnection of people, things and organisations.

A consumer constituting a data subject or group of consumers may be able to institute civil action for damages against a company failing to process personal information lawfully and in terms of section 99 of POPIA. Data subjects have the right to claim civil damages irrespective of the fact that a company has zero intent to contravene the provisions of POPIA.

Companies could face an administrative penalty of up to R10 million or even face criminal prosecution. This is irrespective of a civil action for damages.

Class actions suits are relatively novel in South Africa. This does not mean that it is not a real risk when considering compliance with POPIA. With a class action in the works for the recent listeriosis outbreak, careful consideration should be given as to how these actions can assist victims who suffered on a group scale and to what extent the risk on non-compliance with POPIA can bring about a class action against a company. The 'silicosis' case allowed damages for former mineworkers suffering from silicosis and tuberculosis to be paid by mining companies.

Class actions may well be deemed useful, especially in South Africa, where the majority of the population is poor and would not be able to afford costs associated with litigation.

What can companies do?

Businesses need to prepared for various scenarios. As such, employee training is critical. Having a workforce enabled to protect data could save your company a lot in the long run.

It is not necessarily at executive level where there is a lack of awareness, but indeed at the middle management and grass roots level of companies, where employees do not always understand the full impact of a data privacy breach. We see over and over again that employees still share passwords or create simple passwords such as Abc123.

Compliance with POPIA does not necessarily require the appointment of a group of professional to analyse your company in detail. However, a lean team of professionals together with your own employees can provide the needed insight to guide compliance efforts. Compliance is not a once off event, it is daily vigilance by staff who know the risks and their responsibilities. Core business processes have to be in place and an understanding of duties and responsibilities are non-negotiable.

Until such time that POPIA becomes fully effective, businesses should be paying attention to how they are going to avoid data leaks, civil claims and possible class action suits.



Ahmore Burger-Smidt

Head of Regulatory

View Profile